

ATTORNEY GENERAL OF THE STATE OF NEW YORK  
BUREAU OF INTERNET & TECHNOLOGY

---

In the Matter of

Assurance No. 24-052

**Investigation by LETITIA JAMES,  
Attorney General of the State of New York, of**

**Noblr Reciprocal Exchange, Noblr, Inc., and  
Noblr Risk Management, LLC,**

Respondents.

---

**ASSURANCE OF DISCONTINUANCE**

The Office of the Attorney General of the State of New York (“OAG”) commenced an investigation pursuant to Executive Law § 63(12) and General Business Law (“GBL”) § 899-bb into a data security incident at Noblr Reciprocal Exchange. This Assurance of Discontinuance (“Assurance”) contains the findings of the OAG’s investigation and the relief agreed to by and among the OAG, Noblr Reciprocal Exchange, Noblr, Inc., and Noblr Risk Management, LLC (all Noblr entities collectively referenced as “Noblr” or “Respondents”), whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (Noblr together with the OAG, the “Parties”).

**FINDINGS OF OAG**

1. Many automobile insurance companies provide a quoting tool for use by consumers to generate insurance quotes. These quoting tools are supplied with a data “prefill” capability. When a user enters basic personal details—such as name, date of birth, and/or address—a quote tool with prefill capabilities can automatically populate (or “prefill”) other fields with additional personal information about the person. Quoting tools for consumers are

available on the insurer's public website. Consumers can use these tools to generate quotes as well as purchase a policy.

2. To provide prefill functionality, insurance companies contract with third-party data providers to license consumer data, including the private information of New York residents as defined by General Business Law ("GBL") §§ 899-aa and 899-bb. After a user enters the required data points into the instant quote application, the application transmits the information to the data provider. The data provider, in turn, uses that information to identify the consumer associated with those data points, and then returns additional data about the consumer to the insurer's instant quote application.

3. Depending on the type of data returned, the insurer uses that data to populate prefill fields in the application. These automatically populated fields tend to include information that is relevant in estimating an auto insurance quote, but which the average consumer might not know from memory, including the consumer's driver's license number ("DLN") and vehicle identification number. These fields can also include names and DLNs of additional members of the consumer's household.

#### **Threat Actors Obtained New Yorkers' Private Information Through Noblr's Instant Quoting Tool**

4. Noblr Reciprocal Exchange (the "Exchange") is a reciprocal insurance exchange based in Texas that sells automobile insurance. Noblr Risk Management, LLC, is attorney-in-fact for Noblr Reciprocal Exchange and manages the Exchange's operations. Noblr, Inc. is the sole and managing member of Noblr Risk Management, LLC, and accordingly has supervisory oversight over the Exchange's operations.

5. As part of this business and at all relevant times, Noblr maintained a consumer-facing quoting application on its public website.

6. Noblr's quoting application prompted users to enter their name, date of birth, and address. Not all data points needed to be accurate in order to trigger prefilling. For example, a user who entered an accurate name and date of birth along with an inaccurate address could still trigger prefilling of private information.

7. Noblr's quoting tool exposed consumers' full DLNs in plain text at four different points in its quoting flow: (1) in the source code of the webpage when the prefill function was triggered, (2) on PDF policy application documents generated at the end of the quote, (3) in network traffic when the user submitted payment information to purchase a policy, and (4) on the PDF declaration sent to the user-provided email address upon policy purchase.

8. In January 2021, threat actors discovered that Noblr's quoting tool exposed DLNs in plain text in source code when the prefill function was triggered and used the tool to repeatedly request consumers' private information from Noblr. Using automated means, threat actors were able to acquire approximately 80,000 New Yorkers' DLNs in this manner.

9. On January 21, 2021, Noblr's web team detected a spike in unfinished quotes on its instant quote tool.

10. On January 25, 2021, Noblr began blocking suspicious IP addresses.

11. On January 27, 2021, Noblr determined that the threat actors were scraping DLNs from its instant quote tool. That day, Noblr began masking DLNs in its source code and application documents, at which point the malicious activity subsided.

12. From the time that threat actors began to exploit Noblr's systems until Noblr effectively foreclosed the ability to access additional DLNs, threat actors were able to access and obtain approximately 97,635 DLNs, of which approximately 80,758 were New York DLNs.

13. Many of the New York DLNs acquired as part of these attacks were subsequently

used by threat actors to file fraudulent unemployment claims with the New York State Department of Labor (“DOL”). Although DOL identified many of these fraudulent claims prior to issuing any payments, thousands of fraudulent claimants received at least some amount of unemployment benefits issued in the name of the victims of these attacks.

### **Noblr Did Not Protect Private Information Accessible Through Its Instant Quote Tool**

14. Noblr failed to adopt reasonable safeguards to protect private information that it licensed and transmitted through its computer systems via the quoting tool.

15. As of the time of the incident, Noblr failed to assess the risks associated with its publicly accessible quoting tool that processed private information in the scope of any risk assessments.

16. As a result, Noblr failed to identify that consumers’ DLNs were exposed through the normal and expected use of its publicly accessible web application and did not take steps to protect consumers’ private information.

17. After the breach, a cybersecurity firm identified two other places in Noblr’s quoting flow that exposed full DLNs in plain text: in network traffic when a user submitted payment information and on the PDF declaration sent to the user-provided email address upon policy purchase.

18. Noblr did not authenticate a user prior to retrieving and displaying DLNs in plain text on the face of the application documents and prior to sending a declaration containing DLNs in plain text to a user-provided email address.

19. Noblr did not sufficiently monitor activity on its public quoting tool that processed private information in the course of its regular and expected use. At the time of the incident, Noblr did not monitor site traffic in real time, causing delay in detecting the attack and

difficulty distinguishing between malicious and legitimate activity and identifying affected consumers.

20. After the incident, Noblr implemented additional safeguards to protect consumer private information:

- On February 12, 2021, Noblr masked additional information returned from its prefill provider, including date of birth and vehicle identification number.
- On April 12, 2021, Noblr began requiring the user-entered zip code to match the zip code in its data provider's database in order to move forward in the quote flow.
- On December 15, 2021, Noblr began requiring users of the quoting tool to verify their DLN by entering it manually before allowing the user to purchase a policy.

Noblr also addressed the additional points of exposure and rate limiting issues identified by its post-incident security assessment.

### **Noblr's Violations**

21. Executive Law § 63(12) prohibits repeated illegality in the conduct of any business.

22. GBL § 899-bb requires any person or business that owns or licenses computerized data which includes the private information of a resident of New York to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information. "Private information" includes an individual's name in combination with their DLN. GBL §§ 899(bb)(1)(b), 899-aa(1)(b).

23. The OAG finds that Noblr's conduct violated Executive Law § 63(12) and GBL § 899-bb.

24. Noblr neither admits nor denies the OAG's Findings, paragraphs 1-23 above.

25. The OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12) and GBL § 899-bb based on the conduct described above.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

**RELIEF**

26. For the purposes of this Assurance, the following definitions shall apply:

- a. “API” means application programming interface.
- b. “Biometric Information” means data generated by electronic measurements of an individual’s unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual’s identity.
- c. “Network” means any networking equipment, databases, data stores, applications, software, servers, endpoints, or other equipment or services that are capable of using, exchanging, or sharing software, data, hardware, or other resources and that are owned and/or operated by or on behalf of Respondent.
- d. “Private Information” means (i) information that can be used to identify a New York resident in combination with any of the following: Social Security number, any government ID number including driver’s license number, financial account number including debit and credit card numbers, Biometric Information; or (ii) a user name in combination with a password or security question and answer that would permit access to an online account.
- e. “Security Event” means unauthorized access to or acquisition of Private

Information collected, used, stored, retrieved, transmitted, displayed, maintained, or otherwise processed by Respondent.

### **GENERAL COMPLIANCE**

27. Noblr shall implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of Private Information consistent with GBL § 899-bb.

### **INFORMATION SECURITY PROGRAM**

28. Noblr shall maintain a comprehensive information security program (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of Private Information that it collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes. Noblr shall document in writing the content, implementation, and maintenance of its Information Security Program. The Information Security Program shall, at a minimum, include all of the requirements detailed in paragraphs 31-36 and the following processes:

- a. Assess, update, and document, not less than annually, internal and external risks to the security, integrity and confidentiality of Private Information, including but not limited to all entries in the most recent Data Inventory;
- b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the identified internal and external risks that are appropriate to: (i) the size and complexity of Noblr’s operations; (ii) the nature and scope of Noblr’s activities; and (iii) the volume and sensitivity of the Private Information that Noblr collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes;
- c. Assess, update, and document, not less than annually, the sufficiency of

any safeguards in place to address the identified internal and external risks to Private Information, and modify the Information Security Program based on the results to ensure that the safeguards comply with this Assurance;

d. Test and monitor the effectiveness of such safeguards not less than annually, and modify the Information Security Program based on the results to ensure the safeguards comply with this Assurance;

e. Assess, update, and document, not less than annually, the Information Security Program and adjust the Program in light of any changes to Noblr's operations or business arrangements, or any other circumstances that Noblr knows or has reason to know may have an impact on the effectiveness of the Program.

f. Take reasonable steps to select service providers capable of reasonably safeguarding Private Information, contractually require service providers to implement and maintain reasonable safeguards to protect Private Information, and take reasonable steps to verify service providers are complying with the contractual requirements.

29. To the extent Noblr's cybersecurity is managed by Noblr and not by another entity within its corporate family, Noblr shall designate a qualified employee responsible for implementing, maintaining, assessing, updating, and monitoring the Information Security Program (the "Chief Information Security Officer"). The Chief Information Security Officer shall have the credentials, background, and expertise in information security appropriate to the level, size, and complexity of their role in implementing, maintaining, assessing, updating, and monitoring Noblr's Information Security Program. The Chief Information Security Officer shall report on Noblr's Information Security Program at least quarterly to the Chief Executive Officer (or the equivalent thereof) responsible for the operation of Noblr and at least annually to the



Board of Directors with oversight responsibility for Noblr. Such reports shall be in writing and include but not be limited to the following: the staffing and budgetary sufficiency of the Information Security Program, the degree to which the Information Security Program has been implemented, challenges to the success of the Information Security Program, the existing and emerging security risks faced by Noblr, and any barriers to the success of the Information Security Program.

30. Noblr shall provide notice of the requirements of this Assurance to employees within its corporate family responsible for implementing, maintaining, assessing, updating, or monitoring Noblr's Information Security Program and shall implement reasonable training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within ninety (90) days of the Effective Date of this Assurance, or within forty-five (45) days of when an employee first assumes new responsibility for implementing, maintaining, assessing, updating, or monitoring Noblr's Information Security Program. Noblr shall document that it has provided the notices and training required in this paragraph.

#### **SPECIFIC INFORMATION SECURITY REQUIREMENTS**

31. Data Inventory: Within ninety (90) days of the Effective Date of this Assurance, Noblr shall develop and maintain a data inventory of all instances in which it collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes Private Information. Noblr shall update and document its data inventory not less than annually. The data inventory shall, at a minimum, include the following processes:

- a. Identify all points at which Private Information is collected, used, stored, retrieved, transmitted, displayed, maintained, or otherwise processed;
- b. Map and/or track the complete path of all data flows involving Private

Information, including API calls; and

c. Ensure that reasonable safeguards are used to protect Private Information at all times, including but not limited to reasonable encryption, masking, obfuscation, and other methods of rendering Private Information incomprehensible and/or inaccessible.

32. Governance: Noblr shall maintain reasonable written policies and procedures designed to ensure the security, integrity, and confidentiality of Private Information obtained from a third party.

33. Secure Software Development Lifecycle: Noblr shall maintain written policies and procedures designed to ensure secure software development practices for and regular security assessments and testing of all web-based, mobile, or other applications—whether public-facing, credential-based, or internal—maintained by or on behalf of Noblr that collect, use, store, retrieve, transmit, display, maintain and/or otherwise process Private Information. Such policies and procedures must include the following requirements:

a. Wherever Private Information is implicated by the regular and expected use of any such application, Noblr shall consider the privacy impact at each relevant stage of the software development lifecycle process;

b. Wherever Private Information is implicated by the regular and expected use of any such application, Noblr shall include privacy testing and approval each time the application is changed or updated;

c. For personnel within Noblr's corporate family who develop software used by or on behalf of Noblr, provide periodic education on Private Information, how such information can be used for fraud, and Noblr's procedures, guidelines, and standards for protecting such information;

d. For external software development vendors, comply with Paragraph 28(f) of this Assurance.

34. Authentication: Noblr shall maintain reasonable account management and authentication procedures, including the use of MFA (or a reasonably equivalent control) for access to Private Information.

35. Web Application Defenses: Noblr shall maintain reasonable safeguards to prevent Security Events through attacks on web applications. Such safeguards shall at least include the use of reasonable bot detection and mitigation tools.

36. Logging & Monitoring: Noblr shall maintain a system designed to collect and monitor Network activity as well as activity on any platforms or applications operated by or on behalf of Noblr that collects, uses, stores, retrieves, transmits, displays, maintains, or otherwise processes Private Information. Noblr shall also establish and maintain reasonable policies and procedures designed to properly configure such tools to report anomalous activity. The system shall, at a minimum: (i) provide for centralized logging and monitoring that includes collection and aggregation of logging for Noblr's Network and any platforms or applications operated by or on behalf of Noblr that collects, uses, stores, retrieves, transmits, displays, maintains, or otherwise processes Private Information, and (ii) monitor for and alert security personnel to suspicious activity. Activity logs should be readily accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

#### **OAG ACCESS TO RECORDS**

37. Noblr shall retain the documentation and reports required by paragraphs 28, 29, 30, and 31 for at least six years. Such documentation and reports shall be made available to the OAG within fourteen (14) days of a written request from the OAG. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any other claim.

#### **MONETARY PENALTY**

38. Noblr shall pay to the State of New York five hundred thousand dollars (\$500,000) in civil penalties. Payment of the civil penalty shall be made in full by wire transfer within ten (10) business days of the Effective Date of this Assurance. Any payment shall reference AOD No. 24-052.

#### **MISCELLANEOUS**

39. Noblr expressly agrees and acknowledges that the OAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 47, and agrees and acknowledges that in such event:

- a. any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;
- b. the OAG may use statements, documents or other materials produced or provided by Noblr prior to or after the effective date of this Assurance;
- c. any civil action or proceeding concerning compliance with this Assurance must be adjudicated by the courts of the State of New York, and that Noblr irrevocably and unconditionally waives any objection based upon personal jurisdiction,

inconvenient forum, or venue for purposes of compliance with this Assurance only.

40. If a court of competent jurisdiction determines that Noblr has violated the Assurance, Noblr shall pay to the OAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

41. This Assurance is not intended for use by any third party in any other proceeding.

42. Acceptance of this Assurance by the OAG is not an approval or endorsement by OAG of any of Noblr's policies, practices, or procedures, and Noblr shall make no representation to the contrary.

43. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Noblr. Noblr shall include any such successor, assignment, or transfer agreement a provision that binds the successor, assignee, or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the OAG.

44. Noblr shall contractually require in writing any purchaser, successor, assignee, transferee, or recipient of any Noblr asset that collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes Private Information to comply with obligations equivalent to those required of Noblr in paragraphs 28-37 of this Assurance in connection with the asset.

45. Any failure by the OAG to insist upon the strict performance by Noblr of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by the Noblr.

46. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 24-052, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Noblr, to: Ryan Rist, Assistant Vice President and Head of Noblr, or in his absence, to the person holding the title of Head of Noblr

9800 Fredericksburg Road  
San Antonio, TX 78288-0001

If to the OAG, to: Hanna Baek, Assistant Attorney General, or in her absence, to the person holding the title of Bureau Chief

Bureau of Internet & Technology  
28 Liberty Street  
New York, NY 10005

47. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by Noblr and its counsel and the OAG's own factual investigation as set forth in Findings, paragraphs 1-23 above. Noblr represents and warrants that neither it nor its counsel has made any material representations to the OAG that are inaccurate or misleading. If any material representations by Noblr or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

48. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Noblr in agreeing to this Assurance.

49. Noblr represents and warrants, through the signatures below, that the terms and conditions of this Assurance are duly approved. Noblr further represents and warrants that

Noblr, by Ryan Rist, as the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of Noblr.

50. The obligations set forth in paragraphs 27-37 of this Assurance shall expire at the conclusion of the seven (7) year period after the effective date, except to the extent GBL §§ 899-bb applies to Noblr, in which case paragraphs 27-37 shall apply with full force. Provided, however, that nothing in this paragraph shall be construed as excusing or exempting Noblr from complying with any applicable state or federal law, rule, or regulation.

51. Nothing in this Agreement shall relieve Noblr of other obligations imposed by any applicable state or federal law or regulation or other applicable law. Noblr does not concede that it is subject to New York jurisdiction other than with respect to the terms of this Assurance.

52. Noblr agrees not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis. Nothing in this paragraph affects Noblr's right to take legal or factual positions in defense of litigation or other legal proceedings to which the NYAG is not a party or to otherwise make statements consistent with paragraph 24.

53. Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that Noblr violates the Assurance after its effective date.

54. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

55. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

56. Noblr acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

57. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

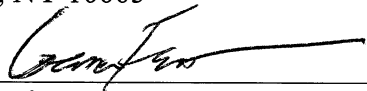
58. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

59. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties, notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

60. The effective date of this Assurance shall be the date the OAG signs this Assurance.




LETITIA JAMES  
Attorney General of the State of New York  
28 Liberty Street  
New York, NY 10005

By:   
Gena Feist  
Assistant Attorney General  
Bureau of Internet & Technology

Date: 12/19/24

Noblr Reciprocal Exchange, Noblr, Inc., and  
Noblr Risk Management, LLC,

By:   
Ryan Rist  
Assistant Vice President and  
Head of Noblr

Date: 8/8/2024

